UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

IN THE MATTER OF THE SEARCH OF: INFORMATION ASSOCIATED WITH DISCORD ACCOUNTS: manny#5739 located on the servers at Discord 401 California Dr Burlingame, CA 94010	Case No. 3:20mj130

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Alexander Hirst, a Special Agent (SA) with Federal Bureau of Investigation (FBI) being duly sworn, depose and state as follows:

INTRODUCTION

1. I make this AFFIDAVIT in support of an APPLICATION for a SEARCH WARRANT under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Discord to disclose to the government records and other information, including the contents of communications, associated with the above-listed account user name that is stored at premises owned, maintained, controlled, or operated by Discord. The information to be disclosed by Discord and searched by the government is described in the following paragraphs and in Attachments A and B.

2. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252A, 2423(b), and I am authorized by law to request a SEARCH WARRANT.

3. This AFFIDAVIT is submitted in support of an APPLICATION under Rule 41 of the Federal Rules of Criminal Procedure for a SEARCH WARRANT for the locations specifically described in **Attachment A** of this AFFIDAVIT, including the contents of the Discord accounts with user manny#5739 (herein after referred to as SUSPECT USER ACCOUNT) that is stored at the premises owned, maintained, controlled, or operated by, Discord, 401 California Dr, Burlingame, CA 94010. Discord is a company that provides remote computing and electronic communications services. This AFFIDAVIT is made in support of an APPLICATION for SEARCH WARRANT to look for contraband and evidence, fruits, and instrumentalities of violations of 18 USC § 2423(b), which items are more specifically described in **Attachment B** of this AFFIDAVIT.

4. The statements in this AFFIDAVIT are based in part on information provided by other law enforcement investigators and on my investigation of this matter. Since this AFFIDAVIT is being submitted for the limited purpose of securing a SEARCH WARRANT, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 USC § 2423(b), Transport With Intent to Engage in Criminal Sexual Activity, are presently located in the SUSPECT USER ACCOUNT.

APPLICABLE STATUTES

1. Travel With Intent to Engage in Criminal Sexual Activity, 18 USC § 2423(b), prohibits a person to travel in interstate commerce with the purpose of engaging in any illicit sexual conduct.

DEFINITIONS

5. The following definitions apply to this AFFIDAVIT and Attachment B:

a. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

b. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

c. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices

(including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

d. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

e. "File Transfer Protocol" ("FTP") is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP, built on client-server architecture, uses separate control and data connections between the client and the server.

f. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and

directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (ISPs) control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

g. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

h. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

j. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

k. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal,

whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

l. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

m. A "website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP").

n. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

DISCORD ACCOUNTS & SERVICES

6. Discord provides free hosting for registered users to set up, configure, and customize their own communication servers, as well as user text chat rooms. Discord is a web-based service which can be accessed via web browser or by installing an application for a Windows, iOS, or Android device. Users register for the service with an email address, username, and password; after registering users have access to all of Discords' features, including voice calls and chat rooms. Discord is an instant messaging service that provides both text and voice communication. Discord conversation logs are saved to a "Chats" area in the user's Discord account. Discord account users can link other social media and entertainment services to their

Discord account and can automatically integrate features of those applications such as Google+. Discord stores identifying information (such as email address used to register an account and a history of IP addresses), and usage information (such as chat logs, login sessions, and device information). Discord also collects information from any third-party application linked to a user's profile. The user account for a Discord account is alphanumeric username, which is then combined with a pound symbol (#) as well as a string of 4 or 5 randomized numbers, producing a unique "tag." The tag is publicly visible on an account's profile and can be used for a variety of networking purposes inside of Discord, such as friend lists, server whitelists, and blocking other users.

PROBABLE CAUSE

7. On April 16, 2020, Union County Sheriff's Office completed a missing person report. The relative of a 14-year-old female victim reported the victim had run away and was possibly in Charlotte with a 26-year-old adult male, later identified as the defendant Manuel Oppenheimer. The relative was able to research the victim's call log via an "AT&T app" and identify the victim's possible location. Charlotte-Mecklenburg- Police Department ("CMPD") responded to an address in Charlotte, North Carolina where the victim and the defendant were located. The victim was subsequently transferred to Union County.

8. On April 17, 2020, Union County Sheriff's Office alerted the CMPD Central Division that the victim disclosed that she had sexual intercourse with the defendant at the address in Charlotte, North Carolina. The victim was taken to the hospital for a sexual assault examination.

9. CMPD Detectives spoke with the victim who confirmed that she had vaginal intercourse with the defendant a few hours earlier on April 16, 2020, in Charlotte. The victim

stated that the incident occurred in the bedroom of an "Airbnb" rented by the defendant.

10. The victim reported she met the defendant on "Omegle," a free online chat website, and communicated using her phone. The defendant's contact information was saved in her phone under a "ring emoji."

11. After the victim's initial disclosure to Union County, CMPD patrol officers returned to the incident address. The patrol officers obtained consent to search the apartment from the defendant. The defendant agreed to voluntarily speak with detectives at the Law Enforcement Center in Charlotte NC 28202. The defendants Samsung, telephone number 929-304-1847 which uses a Google operating system and services was seized by CMPD and a search warrant subsequently executed.

12. The defendant was interviewed and admitted having first met the victim on Omegle before beginning to talk to her on Snapchat, which is a is a mobile native app which allows users to securely share messages, photos, and videos. The defendant stated that he and the victim would "role play" that she was 14 or 15 and he was an older guy. During the course of the Snapchats the victim sent a picture of herself in her underwear to the defendant. This is the only picture the defendant saved on his phone, and this picture was shown to the CMPD detectives. The phone was identified as the same Samsung seized by CMPD.

13. The defendant, who advised that he lived in Brooklyn, New York, stated he and the victim decided to meet now because of the COVID outbreak, otherwise they might have to wait a year before the outbreak ended. The defendant advised that he traveled from New York to Charlotte on April 16, 2020 to meet with the victim.

14. The defendant initially denied having sex with the victim, and stated that the

victim's relative and the police were both calling him for several hours before the victim arrived at his AirBnB. The defendant acknowledged that the police and victim's relative told him that the victim was only 14 years old. Nonetheless, the defendant advised that later in the night, the defendant sent a Lyft to pick the victim up from Union County and bring her to Charlotte.

15. After agreeing to give a buccal swap for DNA to CMPD detectives, the defendant admitted that he and the victim engaged in vaginal penile sex. According to defendant, this occurred after defendant had been informed by numerous times by police and the victim's relative that the victim was only fourteen years old. According to the defendant, he and the victim were only together for about five minutes. Furthermore, the victim stated, the defendant was on the phone with police officers at the time she was at the AirBnB.

16. The defendant was in State custody in North Carolina from April 16, 2020 to April 26, 2020, when he bonded out of the Mecklenburg County Jail in Charlotte, North Carolina. The Defendant was re-arrested by Agents from the Federal Bureau of Investigation late the same day in Charlotte on Federal charges – 18 USC § 2423(b), Transport With Intent to Engage in Criminal Sexual Activity. During post arrest processing, the defendant provided OPPENHEIMER.MANNY1@GMAIL.COM as his contact information. Furthermore, the information matched the e-mail contained on the defendants phone seized by CMPD.

17. Based on a search of the defendants phone seized by CMPD a Discord account was discovered to be associated with OPPENHEIMER.MANNY1@GMAIL.COM, user manny#5739. In a review of chats, a conversation with user mckayladoesntgamex was discovered. The chats took place on or about April 14, 2020. "mckayladoesntgamex" sent "manny" a message "hi baby, wanna call, I took another pic for a perspective". "manny" tells "mckayladoesntgamex" to "call

when u want". On or about April 15, 2020, the defendant booked a flight with American Airlines from New York to Charlotte. Upon review an image sent in the chats, the female depicted appears consistent with the victim and the pose is of a similar nature to images taken by the victim. The victim's name is also "McKayla" and is spelled in the same manner as the user utilizing the "mckayladoesntgamex" discord account.

18. Based on my training and experience I am aware that Discord preserves, intentionally or unintentionally, communications, pictures, and other information which may contain information relating to the defendants intent to travel to engage in illicit sexual conduct. The communication from the defendants account may be backed up and stored information created, leading to possible to recovery of data deleted by the defendant from his device.

19. Based on this information, and the aforementioned interstate methods of communication there is probable cause to believe information is contained at the location to be searched which contain information material to the investigation of 18 USC § 2423(b), Transport With Intent to Engage in Criminal Sexual Activity, described in Attachment B.

SPECIFICS OF SEARCH AND SEIZURE OF DISCORD ACCOUNT

20. Information stored in connection with a Discord account may provide crucial evidence of the "who, what, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. Stored electronic communications, and other data retained by Discord, can indicate who has used or controlled the Discord account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a SEARCH WARRANT at a residence. For example, emails, chat logs, and files interacted with may be

evidence of who used or controlled the Discord account at a relevant time. Further, Discord account activity can show how and when the account was accessed or used. For example, Discord logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses; investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Discord account access, use, and events relating to the crime under investigation. Last, Discord account activity may provide relevant insight into the Discord account owner's state of mind as it relates to the offense under investigation. For example, information on the Discord account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

21. Therefore, the account servers of Discord are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Discord, such as account access information, transaction information, and other account information.

22. Because the WARRANT will be served on Discord who will then compile the requested records at a time convenient to Discord, reasonable cause exists to support execution of the requested WARRANT at any time day or night.

23. Notwithstanding 18 USC § 2423(b) or any similar statute or code, Discord shall disclose responsive data by sending it to: FBI Special Agent Alexander Hirst, 7915 Microsoft Way, Charlotte, NC, 28273; or via email to ahirst@fbi.gov.

CONCLUSION

24. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that the Discord account with user accounts manny#5739 located on servers at Discord, 401 California Dr, Burlingame, CA, have been used to 18 USC § 2423(b), Transport With Intent to Engage in Criminal Sexual Activity, described in Attachment B.

25. Further, there is probable cause to believe that evidence of such criminal offenses may be found in Discord records.

26. I, therefore, respectfully request that that attached SEARCH WARRANT be issued authorizing the search and seizure of the items listed in **Attachment B**.

__/s/ ALEXANDER HIRST___
Alexander Hirst
Special Agent,
Federal Bureau of Investigation

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this 18th day of May, 2020, at 1:00 pm.

Signed: May 18, 2020

David C. Keesler
United States Magistrate Judge

REVIEWED BY: Alfredo De La Rosa, AUSA

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

This WARRANT applies to information associated with the Discord account with user manny#5739 which is stored at premises owned, maintained, controlled, or operated by Discord headquartered at 401 California Dr, Burlingame, California 94010.

ATTACHMENT B

PROPERTY TO BE SEARCHED AND/OR SEIZED

This warrant authorizes (i) the search of the property identified in Attachment A for only the following and (ii) authorizes the seizure of the items listed below only to the extent they constitute the following:

(a) evidence of violations of 18 U.S.C. §§ 2423(b) ("subject violations"); or

(b) any item constituting contraband due to the subject violations, fruits of the subject violations, or other items possessed whose possession is illegal due to the subject violations; or

(c) any property designed for use, intended for use, or used in committing any subject violations.

Subject to the foregoing, the items authorized to be seized include the following:

I. Information to be disclosed by Discord.

To the extent that the information described in Attachment A is within the possession, custody, or control of Discord, including any emails, chats, images, records, files, logs, or information that have been deleted but are still available to Discord, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Discord is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all chats associated with the account, including stored or preserved copies of chats sent to and from the account, the source and destination addresses associated with each chat, the date and time at which each chat was sent, and the size and length of each chat;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between Discord, and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2423(b), including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. All images depicting children engaging in sexually explicit conduct as defined in 18 U.S.C. § 2423(b)

b. All electronic communications regarding children engaging in sexually explicit conduct;

c. All communications with potential minors involving sexual topics or in an effort to seduce the minor.

d. Any evidence that would tend to identify the person using the account when any of the items listed in subparagraphs a-c were sent, read, copied or downloaded.

e. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.